Client system 10 further includes a client identifier 93, which can be a unique number associated with the client system. Client message generator 94 combines client identifier 93, the random number, and the current value of the security count, which indicates the current time. The value of the security count is a time identifier which permits the server system, as further described below, to specify the times at which the client system is to repeat the procedure for verifying the authorization of the server system. The value of the security count gives the server system a reliable understanding of the current time as measured by the client system.

The resulting client message is encrypted by client message encryptor 96 using an encryption key 98. In one embodiment, encryption key 98 is encoded in an integrated circuit, such as ASIC 30 of Figure 2. Encoding encryption key 98 in hardware as opposed to software greatly increases the difficulty of identifying the encryption key by those who might want to compromise the security of the system. In another embodiment, multiple encryption keys 98 can be encoded on the integrated circuit, further increasing the difficulty of learning the encryption key and determining which of the multiple keys is used in any specific instance. When multiple encryption keys are available, the particular key that is to be used can be selected in a random process. In addition, when there are multiple encryption keys 98, the encryption key that is used to encrypt a particular client message can be included in the client message for a purpose that is discussed below in reference to Figure 5.

The encrypted client message is sent from client system 10 to server system 60 via network interface 54. Client message decryptor receives the client message through network interface 55 and decrypts it using the appropriate decryption key 102. When client system

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

10 includes only one encryption key 98, the selection of the decryption key 102 is relatively straightforward, since there will be only one decryption key.

However, when client system 10 includes multiple encryption keys 98, decryption may involve successively applying the corresponding decryption keys 102 to the client message in a trial and error process until one decryption key is found to successfully decrypt the message. Because the client message includes a random number, the security count, and the client identifier, a successful decryption can be determined when the decrypted client identifier matches one of the client identifiers registered at server system 60. It is noted that in some embodiments it may not be possible to reliably determine whether a message has been successfully decrypted by examining only the decrypted random number, and to a lesser degree, the security count, since the server system does not know what random number and security count to look for.

In some embodiments, there can be a very small risk that the client message decryptor 100 will apply one of the decryption keys 102 that does not correspond to the encryption key 98 used by client system 10, but will still determine that the decrypted client identifier matches one of the registered client identifiers. In other words, there can be a small possibility of a false positive decryption, in which the wrong decryption key will process the encrypted client identifier such that, by chance, it matches one of the registered client identifiers. If this were to occur, the random number would not be properly decrypted. Including the encryption key in the encrypted client message can eliminate this risk, however slight it might be. In particular, client message decryptor 100 can successively apply the multiple decryption keys 102 to the client message until the decrypted client message reveals an encryption key that corresponds to the decryption key just applied to the client message and a client identifier that matches a registered client

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

identifier. Nonetheless, for most purposes, the invention can be practiced with negligible risk of a false positive decryption result without including the encryption key in the client message. Indeed, in many cases, the efficiency losses incurred by increasing the size of the client message could outweigh any benefits that might be realized by eliminating the risk of a false positive decryption result.

Once the client message has been successfully decrypted, the message is decombined, or separated into its constituent parts, by client message decombiner 104 using the inverse mathematical operation that has been used to combine these values at client system 10. Client identifier 93, security count 106, and random number 108 are thereby extracted from the client message. In embodiments that establish the authorization level by which client system 10 is to receive service in addition to verifying the authorization of server system 60 to provide service, client identifier 93 is compared against client authorization database 110, which contains records of the authorization levels of the registered clients. The appropriate authorization code 112 for client system 10 is derived from client authorization database 110.

Server system 60 can perform any additional security checks to verify the identity of client system 10. For example, server system 60 can request that client system 10 securely transmit its client identifier 93 to compare it against the client identifier included in the client message. Those skilled in the art will recognize that other information can be transmitted from client system 10 to server system 60 in order to verify the validity of the client message.

Based on the value of security count 106, which specifies the time that the current authorization interrupt has been asserted, as measured by the client system, an expiration count selector 114 selects a new expiration count 116. New expiration count 116 can be

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111